Document Revisions

ENAV18-11.7

Formerly VDES1-12.3.2

***AISM***Association Internationale de Signalisation Maritime ***IALA***

International Association of Marine Aids to Navigation and Lighthouse Authorities

10, rue des Gaudines

78100 Saint Germain en Laye, France

Telephone: +33 1 34 51 70 01 Fax: +33 1 34 51 82 05

e-mail: [contact@iala-aism.org](mailto:contact@iala-aism.org) Internet: [www.iala-aism.org](http://www.iala-aism.org)

**IALA Guideline No. ####**

**On**

**VHF Digital Exchange System (VDES) Operational Concept**

**Technical Annex**

**Edition 1**

**[Date issued]**

**[Previous Edition; Date issued]**

Revisions to the IALA Document are to be noted in the table prior to the issue of a revised document.

|  |  |  |
| --- | --- | --- |
| **Date** | **Page / Section Revised** | **Requirement for Revision** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table of Contents

[Document Revisions (Title style) 1](#_Toc443477599)

[Table of Contents 3](#_Toc443477600)

[Index of Tables 3](#_Toc443477601)

[Index of Figures 3](#_Toc443477602)

[Guideline on VHF Digital Exchange System (VDES) Operational Concept 4](#_Toc443477603)

[ANNEX A VDES Technical Guideline 4](#_Toc443477604)

Index of Tables

[Table 1 Title required 4](#_Toc216488847)

Index of Figures

[Figure 1 Title required 4](#_Toc216488874)

Guideline on VHF Digital Exchange System (VDES) Operational Concept

1. VDES Technical Guideline
2. Background

ITU has recognised the efficiency and the necessity for digital communications, has produced technical standards and has revised the VHF marine band (RR Appendix 18) to designate channels for data transmission. It is recognized that both analog voice communications and digital communications will share the band. This annex illustrates how the design and installation of the new VDES (Figure 1) should address the compatibility and interoperability of both systems. The VDES, as envisioned by IALA and presented to ITU, addresses the identified need to protect AIS along with essential digital communications contributions for e-Navigation and GMDSS Modernization.

The VHF marine band (Appendix 18 of the International Radio Regulations) was initially used for transmission of voice communications by FM (frequency modulation of the carrier) on 25 kHz channels. The ITU (International Communications Union) introduced the first marine data transmission system, DSC (Digital Selective Calling) in accordance with Recommendation ITU-R M.493, to help ensure that calling and distress communications attempts were successful. VHF DSC transmits data at 1200 bits per second using digital two-tone FSK modulation, slow by modern data standards, but very robust. At the request of the IMO (International Maritime Organization), to improve safety of navigation, ITU introduced another VHF data transmission system, the AIS (Automatic Identification System) in accordance with Recommendation ITU-R M.1371, which provides navigation and identification data for ships, shore stations, aids to navigation and search and rescue devices at 9600 bits per second using digital GMSK modulation.

At the request of some Administrations, to improve spectrum efficiency for VHF Data Exchange (VDE), ITU introduced a standard, Recommendation ITU-R M.1842, with options for 25 kHz, 50 kHz and 100 kHz channels at data rates up to 307.2 kbps using digital modulation waveforms that had been proven by ETSI (European Technical Standards Institute). Appendix 18, in its current revision by the World Radio Conference 2012 (WRC-12), approves all three data transmission methods in accordance with the approved ITU standards (Recommendations ITU-R M.493, M.1371 and M.1842) and designates channels for their use. Consequentially, both voice and data communications now coexist in the VHF marine band.

Consequential to WRC-15, the ITU standard for VDES, Recommendation ITU-R M.2092-0, was approved. Remaining outstanding issue is the approval of the satellite component for the VDE channels which is targeted for approval at WRC-19.

**2020**

**2021**

**2018**

**2019**

**2016**

**2017**

**2022**

**2023**

VDES Terrestrial Initial Operational Capability

VDES Full Operational Capability

AIS

VDE-SAT DOWN

VDE

VDE + ASM

VDE + ASM + SAT

VDE

ASM 1  
ASM 2

ASM-SAT UP

AIS + VDE Terrestrial Initial Operational Capability

Today

AIS 1  
AIS 2

Voice VHF discontinued on January 1st 2017 on ASM and VDE channels

Introducing VDES is expected to happen through 4 operational phases:

1. Today: AIS exists as defined by ITU.R M.1371-5 on the AIS frequencies, and Coastal Stations use the ASM and VDE frequencies for Voice VHF.

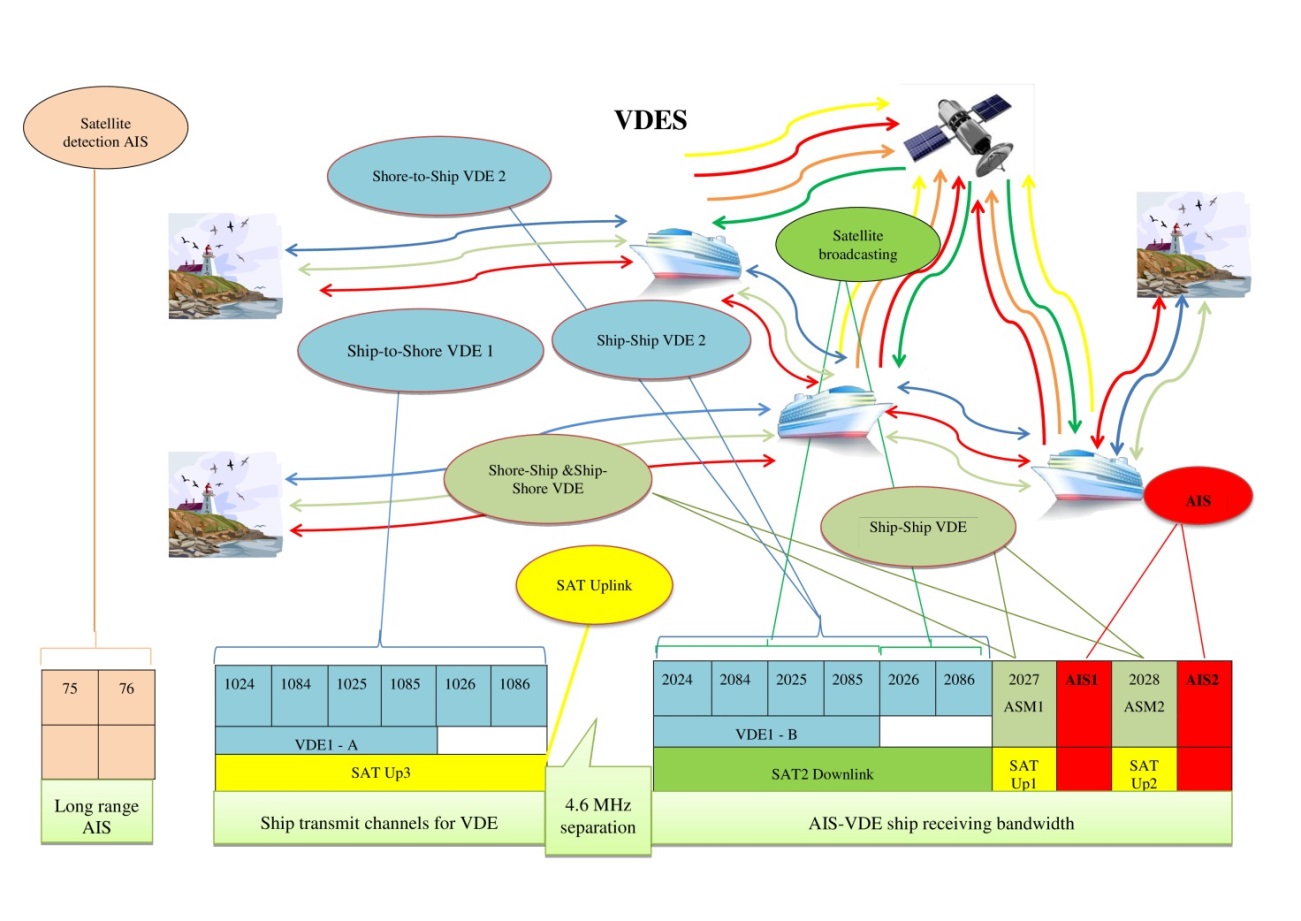
2. Past WRC15 - AIS+ASM: Regionally, where there is an urgent need for offloading the AIS VDL from significant ASM traffic, it is recommended to allow the introduction of 4-channel AIS + ASM devices. These devices may receive and transmit ASM on the ASM1 and ASM2 frequencies, using the existing GMSK modulation defined for AIS, but shall discontinue their transmit capability after January 1st 2019 unless a software upgrade enables them to participate in the modulation and access scheme agreed for the ASM frequencies, when the final VDES recommendation is introduced. Note that the ASM frequencies will need to be shared with the VHF voice service from Coast Stations in many areas.

3. It is foreseen that the when the VDES is finalized, Initial operational capability can be established quickly after January 1st 2019, replacing any GMSK modulation on the ASM1 and ASM2 frequencies, and introducing terrestrial VDE. Note that both the ASM and VDE frequencies will still need to be shared with the Voice VHF service in many areas.

4. When a satellite service is developed, full operational capability of the VDES including the Satellite frequencies can be achieved. Past January 1st 2017, the ASM, VDE and SAT frequencies should not need to be shared with the Voice VHF service

1. VDES Frequencies

VHF data exchange system (VDES) considers Recommendation ITU-R M.2092-0, including both terrestrial and satellite components. Recommendation ITU-R M.2092-0 protects the integrity of the AIS VDL by moving ASMs to other channels. The VDES integrates the functions of AIS, ASM and VDE and includes the channels used for these functions. Appendix 18 of the International Radio Regulations (revised by WRC-15) specify the use of the frequencies for VDES.



It should be noted that the ITU standards for data transmission in Appendix 18 identify the specific channels for data transmission and specify the timing of and maximum time durations for data transmissions. This level of specificity, e.g., the selection of the channels, the timing for the transmissions and the maximum durations of the transmissions, etc., is needed to preserve the integrity of both the data service and the other services in Appendix 18, including the GMDSS. Noting that AIS, DSC and voice communications have been successfully operating in Appendix 18 along with the GMDSS for many years, it was understood that VDES will also be successful if it is implemented in accordance with ITU standards. Taking these matters into account, WRC-15 approved the standard for VDES, Recommendation ITU-R M.2092-0.

1. VDES Services

Deciding to implement a VDES service follows the following decision matrix:

Are sufficient funds available?

Yes

Yes

Yes

No

No

No

Implement VDES services

Are more funds available?

Human resources required

New facilities and equipment

Existing facilities and equipment

Redefine services to be provided

Plan integration of VDES with AIS

Define services to be provided

Continue to use AIS

Keep under review

Is there a need to use VDES?

The following table assists in making this decision:

| **Consideration** | **Detail** | **AIS recommended** | **VDES recommended** |
| --- | --- | --- | --- |
| AIS system load | AIS system load  (see measurement technique in note 1) | <50% load | >50% load |
| Application Specific Messages | Application Specific Messages (ASM) are delayed beyond that acceptable to the users  (see note 2) | Service Latency acceptable | Service Latency not acceptable |
| Advanced data transfer services | If the Advanced system data transfer features are required as per the Maritime Service Portfolios | Not required | Are required |

**Note 1:** System load is determined by measuring the number of vessels in the coverage area of an AIS base station (a single slot map) and calculating the sum of the slots consumed in the coverage area based on the expected reporting rates of the vessels in the coverage area (Class A, Class B, AtoN and AIS base station) and the number of Addressed Binary Messages (ABM) and Broadcast Binary Messages (BBM) of all types.

**Note 2:** Service latency is defined as the delivery of the total service from the initiation of the delivery of the service component to the completion of the delivery of that service component e.g. a single maritime chart update.

The services offered by a VDES system will allow for priority with essential services / safety related services having the highest priority and non-essential / commercial service having the lowest priority.

**[VDES has no defined method of managing transmitted message priorities (e.g. priority 1 to 32 essential services and 33 to 64 for non-essential services). Priority will be implemented at the application layer with the VDES base station having limited message buffering capability and thus not requiring any priority mechanism]**

**[VDES has no defined method of managing presented load. This is to be added to the bulletin board with the bulletin board announcing which traffic can be presented at any particular time. This could be priority based (e.g. priority 1 to 32 essential services and 33 to 64 for non-essential services) or simple essential versus non-essential services based]**

The transfer of data using VDES should consider that the available VDES data transfer capacity is shared by all users within the coverage range of a VDES base station. Data transfers are recommended to be limited to messages that can be transferred within 1(?) second within the system being used (channel bandwidth, modulation type and base station design dependent).

**[The data transfer capacity can be increased by deploying addition VDES base stations with smaller coverage areas (i.e. lower antennas / sectorised antenna systems)]**

* 1. Bulletin Board Support for VDES Service

Shore/Satellite Bulletin Board

* its version,
* valid period
* plans for future changes,
* back up frequency/ back up logical channel for bulletin board tx,
* capability, e.g. modulation, bandwidth, tx capability
* slot usage
  + announcement,
  + data downlink,
  + data uplink,
  + dedicated capacity (slots) to users,
  + slots for random access,
* Satellite orbital parameter
* Area definition:
  + satellite in view,
  + availability of bass station, e.g. condition
  + definition of RF coverage area
  + definition of service areas
* identification of competent authority/operator
* Base station ID

Bulletin board is transmitted on logical channel (e.g. in 5 slots at the beginning of the frame) either on:

* VDE channels
* ASM channels or
* AIS channels

Bulletin board is transmitted using the most robust modulation scheme

Bulletin board coordinates all transmissions between

* Ships (duplex mode)
* Ships to base station
* Base stations
* Authorities
* Countries
* Satellite

Ship to ship communication

Ship to ship in shore coverage area of a base station

* Controlled by base station (dedicated slot usage)
* Autonomous except where restricted by base station
* Mixture of controlled and autonomous in shore coverage
* subject to satellite transmission schedule (shore station should take into account satellite availability)

Ship to ship outside the shore coverage area of a base station

* always autonomous but subject to satellite transmission schedule

Ship to Shore Broadcast

* Possibly use ASM to inform shore of capabilities

1. Integrity monitoring and authentication

Refer to ANNEX 1 and ANNEX 2 (method to be discussed and eventually decided).

1. VDES Shore Infrastructure Considerations (physical/logical)

The VDES base station ends at the OSI level 5 of the OSI 7 layer model (<https://en.wikipedia.org/wiki/OSI_model>). The VDES base station connects to a Base Station Controller (BSC), a VHF antenna system and a timing source (GNSS or other timing source of similar or better accuracy). The VDES base station will connect via a BSC to a system that could follow the Common Shore-based System Architecture (CSSA) structure as described in IALA guideline 1114.

The AIS, ASM and VDE could be separate physical units or could be combined into a single physical unit.

One or more VDES base stations comprising of an integrated base station or a number of separate but connected units can be connected to any one BSC.

AIS

ASM

VDE

BSC

CSSA

AIS

ASM

VDE

External services and applications

The interface between the VDES base station and the BSC will be compliant with IEC 61162-450. The application will route messages to the respective AIS, ASM and / or VDE transmitters based on the communications capability of the vessel as declared by the vessel from time to time. The current AIS Application Specific Messages are described in IMO Circular S/N 289. These Messages, ITU-R M.1371 International Function Messages, and other regional Application Specific Messages are catalogued on the IALA website as Application Specific Message (ASM)(International and Regional).

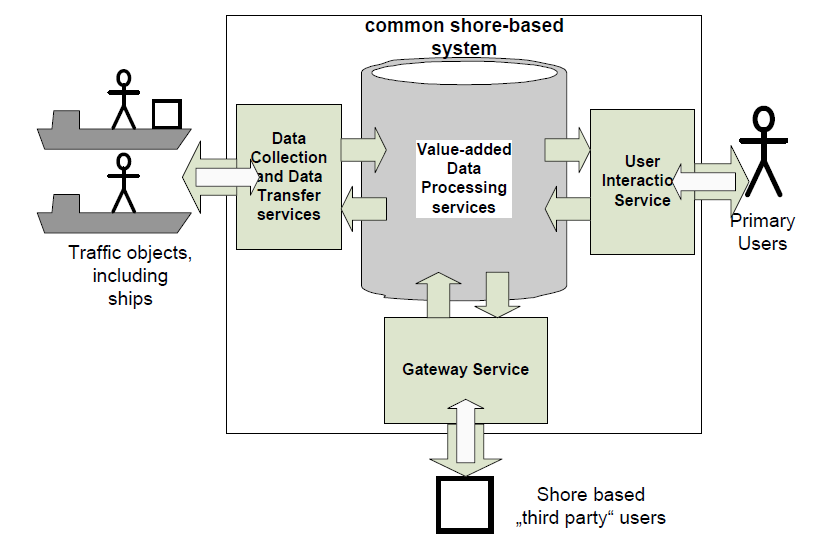
VDES Application Specific Messages shall be treated the same way as AIS Application Specific Messages.

The timing source, although normally a local GNSS system, can be any timing source that has the required accuracy to maintaining the required slot timing accuracy (11uS (?)). If the timing source is lost to the VDES base station, a local timing source could be used provided that the drift of this timing source ensures that the slot timing accuracy with reference to GNSS time is maintained within the specified limits.

When constructing the VDES base station site, the location of the VHF antenna should be accurately known and used for all location based references to that VDES base station.

* 1. CSSA compliant system

The VDES BSC is connected to a CSSA system as described in IALA Guideline 1114. The CSSA model is illustrated below.



The primary users are the users of essential services. The third party users are lower priority user and / or commercial users.

* 1. VDES system capability determination

Both the ship and shore need to have a common record of the communications capability of each side to enable the most effective communications method to be used. This is achieved by both the ship and the shore side systems publishing their respective capabilities from time to time using the bulletin board. This bulletin board can also be polled for by either side when required.

The bulletin board is available on both AIS using an Application Specific Message or via the VDE channels. Where both the ship and shore have overlapping services then these services can be used for the exchange of data.

**[The bulletin board message format and transmit rates need to be agreed and referenced here (one transmission per VDES base station with an interval minimum of one minute and a maximum interval of six minutes to align with AIS). This needs to include the definition of the AIS Application Specific Message contents. Where an AIS base ship or shore side station does not have VDE capability, this could be indicated positively by a flag being clear or historically by this same flag bit now having to be clear in the AIS ITU R M.1371-5 type 4 message. Two of the spare nine bits are recommenced for use. Bit one of the spare bits to indicate ASM capability and bit two of the spare bits to indicate VDE capability.]**

The application (‘value added data processing services’ in the CSSA guideline) will determine the message priorities to be transmitted. The VDES base station will have a minimal buffer and will not need to have the capability to determine VDES message priority and / or change message transmission slots to take account of message priorities.

The authority implementing the VDES base station will need to keep the shore station VDES Bulletin board updated as to services available and offered by the shore side VDES infrastructure. The bulletin board updates could either be by automatic or manual methods.

* 1. Message addressing

VDES messages are sent ship to ship, ship to shore and shore to ship. All addressed messages to ships are directed to a particular ship using that ships MMSI. All broadcast messages for a particular service area are addressed to one or more VDES base station MMSIs.

When messages are sent from the ship to the shore and where the shore side service has an MMSI (refer dynamic MMSI in AIS services), the message will be delivered to the service identified with that MMSI. These are normally primary users (e.g. national coast guard)

Where the shore side service does not have an allocated MMSI, the message will be delivered to the VDES gateway using a global VDES Gateway MMSI and the VDES Gateway will extract from the message the identity of the service that is to consume the message from the ship.

**[The VDES Gateway MMSI is to be agreed and published]**

**[The method of including the identity of the service that is to consume a message is directed through the VDES Gateway service needs to be determined. One method could use X (9?) alpha numeric characters as a ID and this ID would be globally unique and would allow the URL of this service to be looked up on a local Dynamic Naming Service (DNS) (e.g. Gateway\_MMSI.Service\_ID = 123456789.abcdefhij). This requirement needs to be referred to / discussed with the IALA working group dealing with this matter.]**

Vessel

VDES

BSC

CSSA

CONSUMER

URL of Service Provider

MMSI of Vessel

MMSI

ID

DNS

Vessel

Location

Register

AIS

ASM

VDE

BSC

CSSA

AIS

ASM

VDE

VLR

DNS

External services and applications

* 1. Shore based infrastructure

VDES at the OSI Layer Model

VDES Service ends at session layer level 5 OSI Model

Rec ITU-R M.2092 ends at level 4

Single base station VDES shore infrastructure

• Antenna VHF + GNSS

• Antenna cable

• VDES Transceiver

• VDES base station controller,

• Interface to applications IEC 61162-450

• application

adding a second or more base station

VDES base station controller can run n number of VDES base stations

Base station may consist of separate (several) transmitter (tx) and receiver (rx) components

e.g. one tx several rx component

* 1. Timing source with certain level of accuracy

Synchronization may be done via GNSS or by other means

Synchronization timing accuracy xxx

Retain timing for so long time (drift, etc.)

Direct or Indirect synchronization to AIS or others

If sync is not available -> stop transmission

Location of VHF antenna is needed

simultaneous tx by several base stations in the service (single frequency network) is not envisioned

* 1. Architecture of the VDES

VDES-Port (router)

VDE can use existing infrastructure from AIS,

Replace the box, interface, etc. is the same

Uplink, downlink to the maritime cloud

All specifications according for shore stations CSSI apply

* 1. Integration

Integration on interface level (one VDES router)

No integration on VDES components level (AIS, ASM, VDE)

Radio: single tx or multiple tx with one antenna or separate antenna

Provide examples for different solutions of the physical infrastructure

How do you provide data to the shore infrastructure

• how do I know ship has VDE

• how do know the right application is onboard

• how do I know that the information is consumed correctly (display update of buoy)

ASM/VDE messages needs applications to be transmitted (generate message) and received (display)

ASM/VDE messages are standardized

Applications are part of the service provision

Publication of ASM/VDE message capability by shore authority

* 1. Essential services / non essential services

Safety services

Commercial services

* 1. Pre-formatted Binary messages(ASM, VDE messages)

defined ASM: IMO Circ. SN 289 , ASM housekeeping, regional ASMs

* 1. Capability request for ASM/VDE messages

• Autonomous transmission of ASM/VDE capability by vessel

• Vessel polls shore infrastructure (port/authority) regarding capability available

• Bulletin board (ASM) contains the ASM/VDE capability of the shore infrastructure (port/authority) or give an index where to find the capability

• Different ASM/VDE service level of a port (1, 3, 4 …)

• Central registry for ASM /VDE messages at IALA (add a new page to existing IALA registry)

Registration process in place (IALA + national authority)

ASM/VDE messages

• ASM/VDE messages have version indicator, e.g. version, sub version, revision of service level

• Ownership of ASM is by the authority

* 1. Non-pre-formatted Binary messages/proprietary ASM/VDE

• one or more specific ASM/VDE message type for non-pre-formatted binary data (data container)

• Different priorities (different message types define priority)

• Commercial/private messages

* 1. Priority

• Application decides about priority

• By message types (base station has to deal with priority upon the message type)

• Embedding priority in the messages (base station has to deal with priority)

• Scheduled messages

• Service jitter (delayed due to priority)

• Add time with the ASM delivery to the base station (knowledge about delay)

* 1. Bulletin board for specific service areas

• Rule set for conflicts e.g. terrestrial and satellite

• set time slot aside for bulletin board

• Bulletin boards tx planning (similar to FATDMA planning, 120 nm rule, RF coverage in the bulletin board)

• Bulletin board has to be decoded by the VDES station, not only by application, as there is information for the VDES station in the bulletin board

• How many bulletin boards stored and act upon (6 or 18 or 32) at the receiving station?

• How long is bulletin board valid?

• How long is bulletin board data wise?

• Default bulletin board for outside the shore station service area: defines default random access slots

• Bulletin board tx once per minute (max) or less in low traffic area?

• Not all information may be included in all bulletin board messages (e.g. geographical area)

system bulletin board document for terrestrial and satellite published by IALA

Three controlling functions for the VDL available

• Bulletin board is static, it is small - Definition of channels, e.g. announcement channel

• announcement channel highly dynamic most information of base station

• Random access control channel - Default configuration for outside the control area

Needed:

Definition ship to ship slots

Definition ship to shore slots

Two set of data:

From shore to ship

From ship to shore

* 1. Application layer

Connect at the base station (not allowed)

Connect at the application layer (application layer set priority)

* 1. Addressing scheme

• Message type

• Address (MMSI, other ID inside the message)-> see Maritime Cloud

Requires liaison with ITU (Rec M.585) to accommodate access to the MC.

**ANNEX 1. Integrity monitoring and authentication for VDES - Tokyo Workshop Output**

Bulletin Board Messages are crucial for the operation of VDES Services. Attacking those messages can be highly attractive for the attacker as the number of consecutive services and the number of affected people is supposed to be significant. As the channel capacity is limited security here is a balance between effort/efficiency and effectiveness. The shared media radio can be harmed by jamming as soon as economic capacity is given which identifies hints for the upper level of security (more operational safety) that can be achieved. On the other hand by it shall be prevented to harm valuable services by just making use of a simple notebook in combination with a ham radio initiated by a “script-kiddy”.

For this purpose a message authentication concept where the public keys are distributed via a public key infrastructure is proposed.

Initiation of the network of trust is given as each ship borne VDES equipment trusts the named root certification authorities (“1”). This information is initially programmed into the devices in a similar way like mobile devices (and desktop browsers and operating systems) trust e.g. “VeriSign Universal Root Certification Authority”. Once the root certificates are available each certificate signed with one of the trusted root certificate on top of the chain is part of the network of trust. Those certificates will be published either via the BB Channel or the announcement channel. Downloading the certificates can/should be performed as long as the vessel is within LTE/3G/WiFi coverage area by making use of those broadband / cost effective channels (“2”).

Publisher of a bulletin board message signs the message to be issued with his private key by the use of the one-way-hash-function (“3”). Even if strong hashing is in charge (SHA-2 with 256 Bits or even SHA-3 with 1600 Bits) the message authentication header is truncated to the 4 least significant bytes before transmission. This truncation provides the balance between adequate security and overhead.

Open here: are 4 Byte the proper balance?

The ship receiver can verify the message authenticity by checking the integrity with the issuer’s public key (“4”).

Open here: how in detail to incorporate the public key to the certificate?

As the bulletin board message is authenticated but not encrypted as a fall-back the receiver simply can trust and interpret the plain message when cryptographic system is either not applied at all or simply not working. Certificates for a certain service area and Certificate Revocation List has to be broadcasted via a public channel (Open here: BB Channel or announcement channel) as well (“2”). Certificate Revocation List is needed once a certification authority was compromised and all its issued certificates have to be revoked immediately. Compromising a certificate authority should happen rarely which results in a very short list.

Whether to make use of the public internet root certificate authority or to establish dedicated root authority within IALA organisation has to be decided. There are pros and cons for both approaches namely:

• Independence of any 3rd party provides autonomy for our application

• Reusing well established business processes and organisations on certificate handling can reduce effort and costs



**ANNEX 2. Integrity monitoring and authentication for VDES - Pre-Distributed Public Keys**

# Summary

This paper proposes a method for delivery of keys required for authentication of application data transmitted over VHF Data Exchange System (VDES).

# Background

The IALA VDES Workshop organized in Tokyo 15-19 February 2016 noted that Cyber Security is an important matter to be considered for the VDES and further considered that it is necessary to agree on a mechanism for authenticating the source of information that is transmitted by using the VDES.

The workshop further developed a draft technical annex for the envisioned future IALA guideline on VDES. This draft technical annex contains a proposal for the provision of means for Cyber Security in form of both PKI and using certificates in building the line of trust.

# Discussion

While appreciating the discussion and output at the IALA VDES Workshop in February 2016, as a continuation of the discussion, we propose to amend the method of authentication by implementing use of pre-distributed public keys.

Target of this proposal is authentication of payload for VDES related applications transferred over the VDES. Authentication of the Bulletin Board of the VDES is a separate issue – it may need or not need authentication. If the Bulletin Board needs authentication, it could be based on ideas introduced in this document or on some other idea.

The particular motive for our suggestion is to keep the standard method of authentication compatible with all methods of existing and future marine communications.

In detail, to our experience an automatic on-line check for a chain of trusted certificates may become restrictive from the compatible communication methods point of view due to the related latency issues typical for maritime communications between ship and shore.

The mechanism of authentication by using pre-distributed public keys as proposed in this paper has been proven feasible in the distribution of Electronic Nautical Charts (ENC), including online updates (See IHO S-63).

The application of the proposed method for Shore-to-Ship, Ship-to-Shore and Ship-to-Ship transactions is briefly described in following Figures 1 to 4.

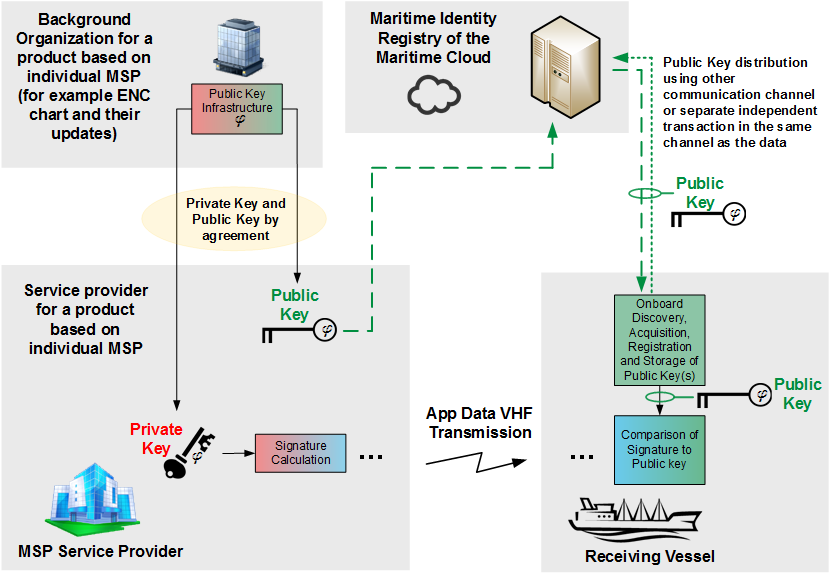


Figure 1 Public Key pre-distribution for authenticating Shore-to-Ship Official MSP transaction application data

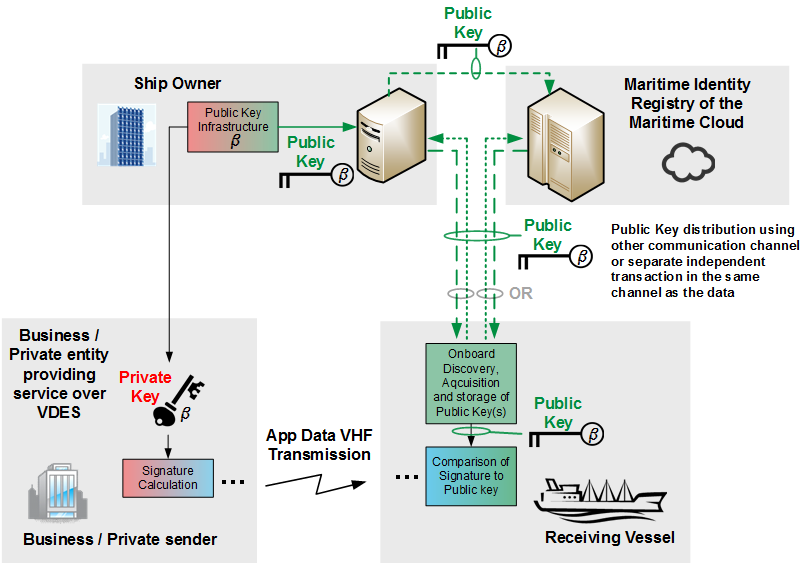


Figure 2 Public Key pre-distribution for authenticating Shore-to-Ship business / private transaction application data

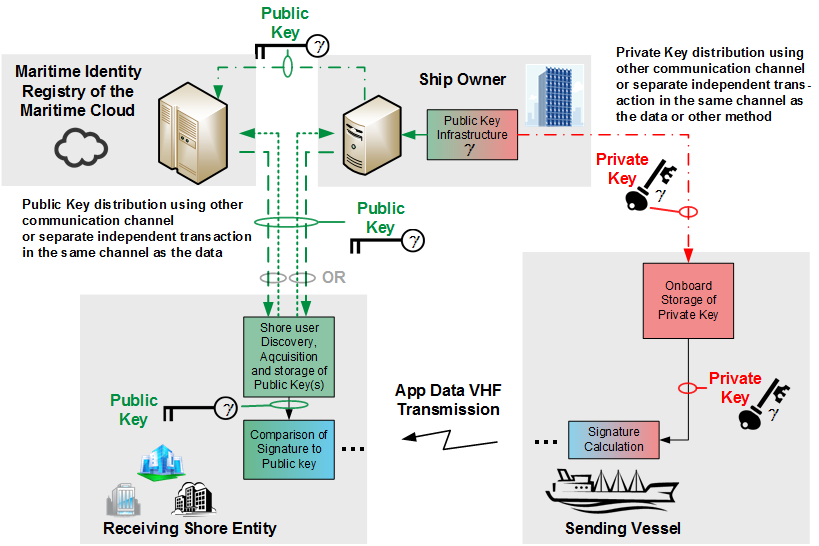


Figure 3 Public Key pre-distribution for authenticating Ship-to-Shore application data

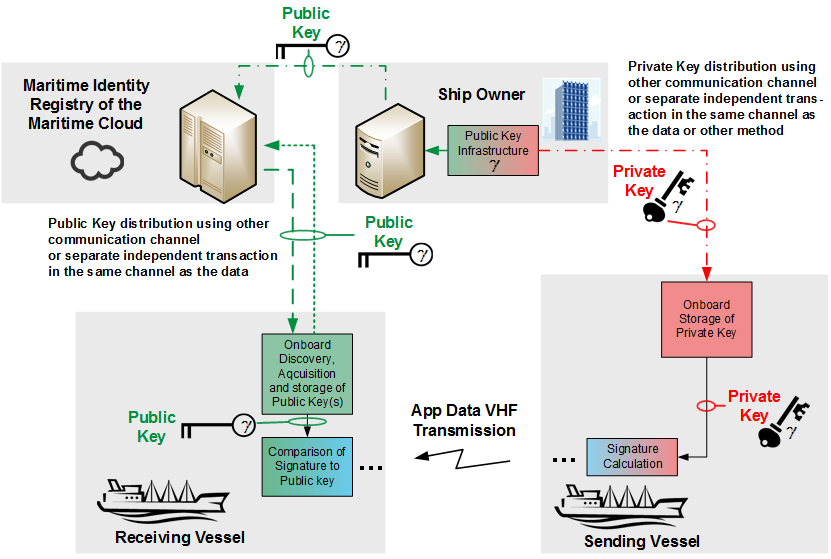


Figure 4 Public Key pre-distribution for authenticating Ship-to-Ship application data

**Properties:**

(1) Pre-distribution of Public Key(s) can be carried out by any standard communication means including VDES. If VDES is used for transfer of the keys, then the related communication session should be arranged separately from transfer of the payload. Adopting a standardized electronic key-interchange format could assist in inputting the Public Keys to ship equipment. Alternatives for a distribution format could be at least IHO S-63 pub, X.509 or email signature. One obvious source of the pre-distribution of the public key(s) could be the Maritime Identity Registry of the Maritime Cloud.

(2) If the keys in use are compromised, a new Public Key could be transmitted by using any available standard marine communications method. Data consumer application would just recognize that installed key no longer matches to the signature of the received data and would prompt user about the detected discrepancy. User could then have option to temporarily trust received data, install new key or discard the received data. Application could offer a wizard for requesting new key and installation of it.

**Recognized further items to discuss/develop**

(a) Adoption for different Public Keys of different instances requires simultaneous handling of multiple public keys by the shipborne VDES related applications. This detail should be included into the IALA Guideline on user requirements for VDES related applications.

(b) There should be an easy way to input the Public Key, received by other means than VDES, into VDES related application in any shipborne equipment. This could belong to a function of registering VDES related application for a service. Also this detail should be included into the IALA Guideline on user requirements for VDES related applications.

* For example every ECDIS is required to have two independent methods for entering the Public Key for ENC charts and their updates. First method is based on a file in "IHO S-63 .pub"-format or in X.509-format. Second method is based on manual input of the character string representing the Public Key. The second method can be used if the first method is not possible, the related text string could have been received by any method supporting text (for example Navtex, email, voice, etc.)

(c) Each instance providing VDES related application services could either establish own PKI or agree to use some existing PKI provided for example by the competent international body (for example IHO, IALA, etc.), by an administration of the country the service instance is registered to or by a ship owner (especially for use cases when a ship is source of data). Also this detail should be included into the IALA Guideline on user requirements for VDES related applications.

* For example IHO has provided Public Key infrastructure for all publishers of ENC charts and their updates. The Private Key have been provided by IHO for data source based on written agreement between data source and IHO. The Public Key has been available for downloading from web-page of IHO. Typically ECDIS manufacturers have preloaded this Public Key into their ECDIS before delivery to the customers.

# References

1. IHO Publication S-63: IHO Data Protection Scheme, Ed 1.2.0, Jan 2015